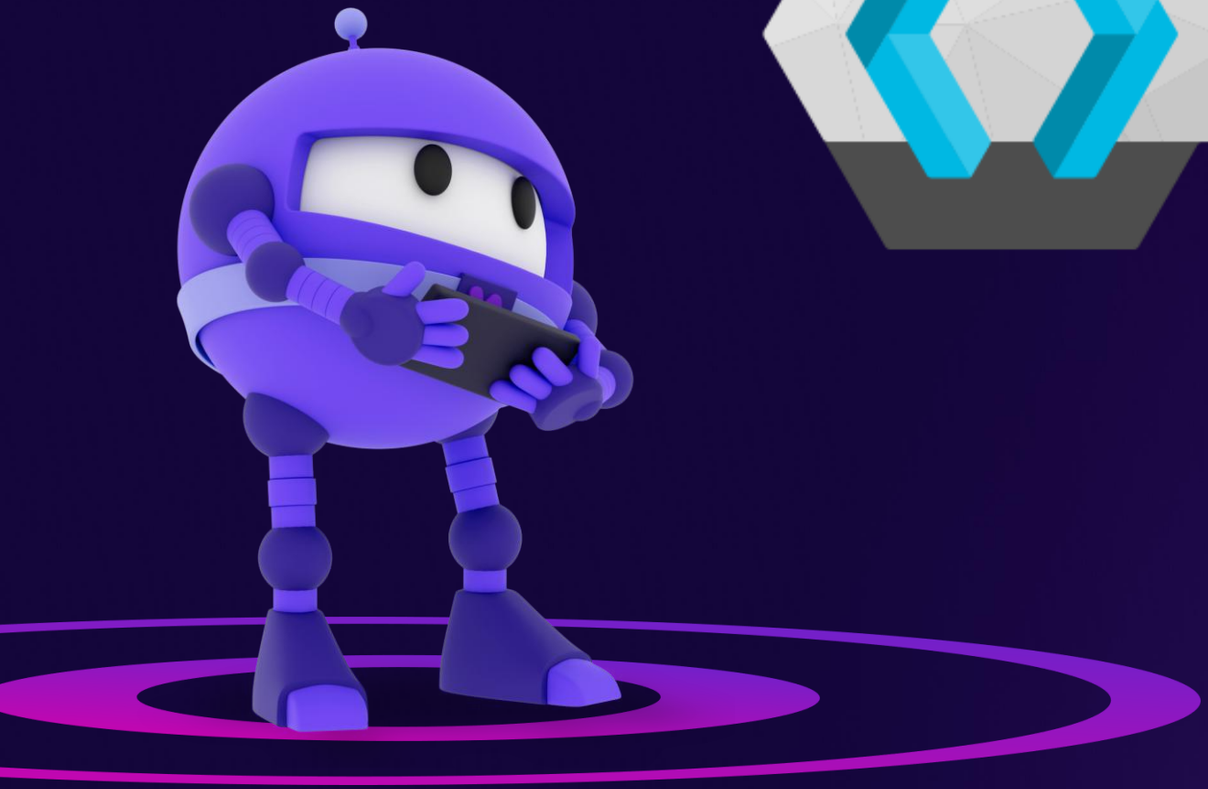
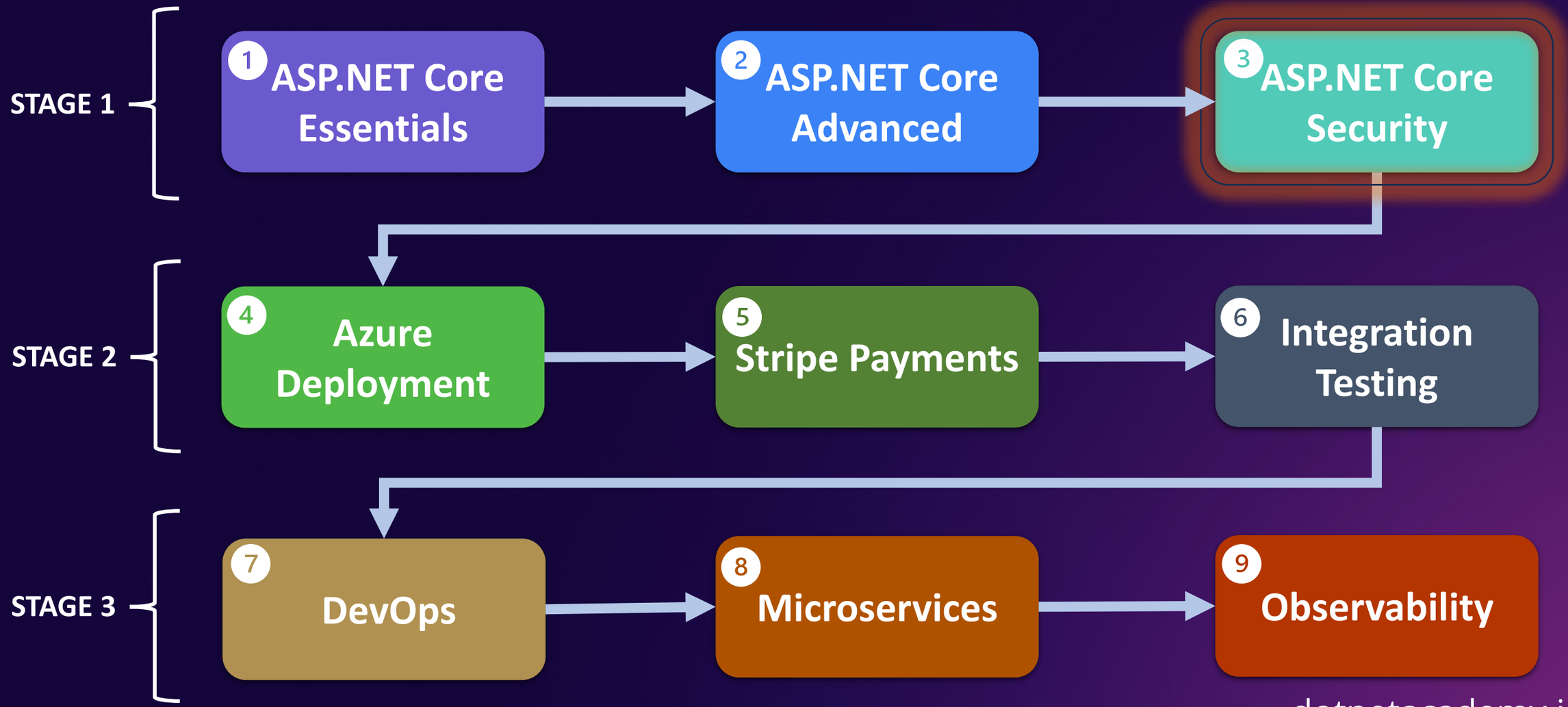
3. ASP.NET Core Security



Where are we?



dotnetacademy.io

ASP.NET Core Security Topics

- Authentication
- Authorization
- Using Docker Images
- Users and Roles with Keycloak
- OAuth 2.0
- ASP.NET Core APIs + Keycloak
- OpenID Connect
- Secure Front-end with OIDC

What you need to know first

- **ASP.NET Core REST APIs**
- **Dependency Injection**
- **Working With Data (EF Core)**
- **Configuration System**
- **Middleware**
- **Logging**
- **Using Postman**

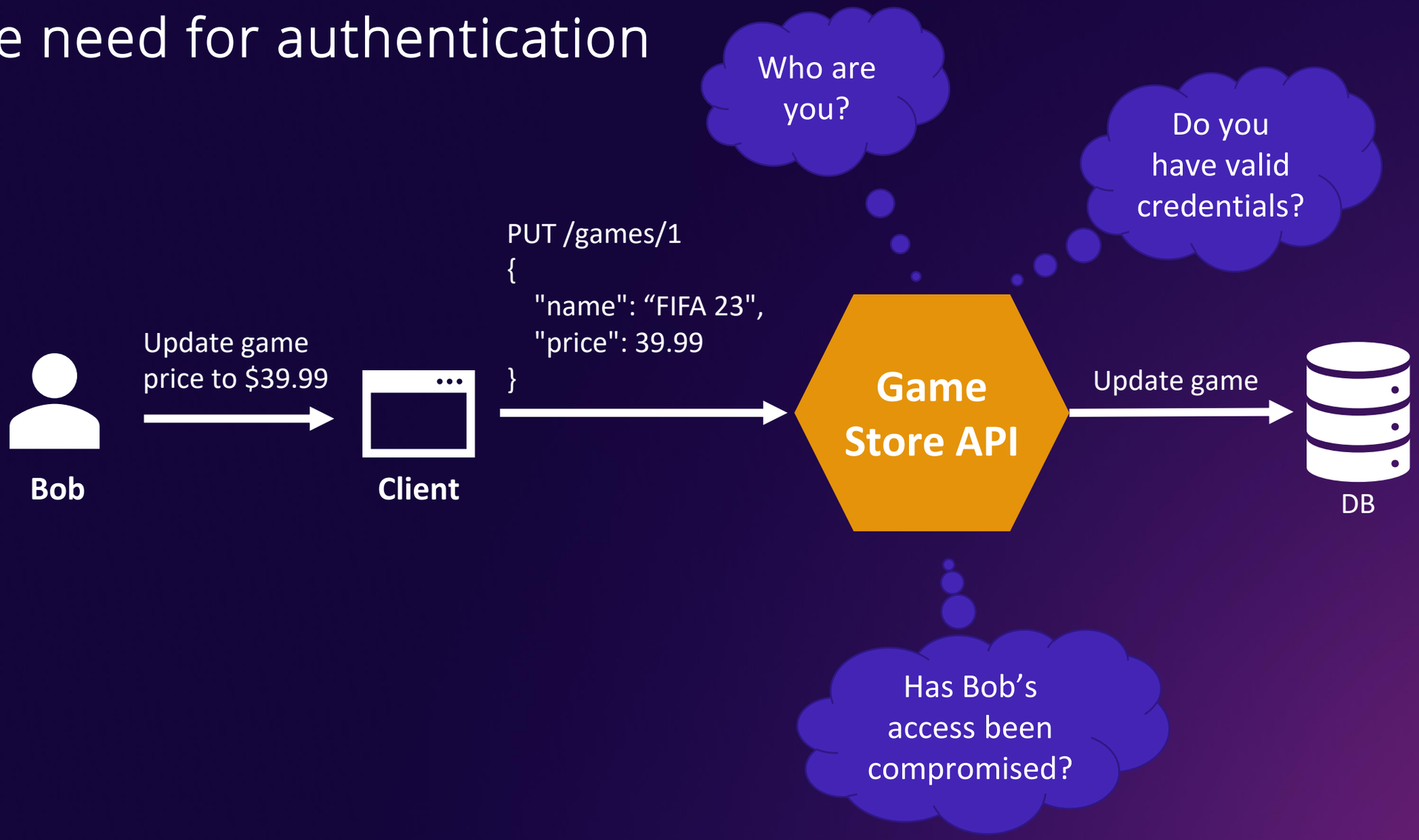
dotnetacademy.io

Software prerequisites

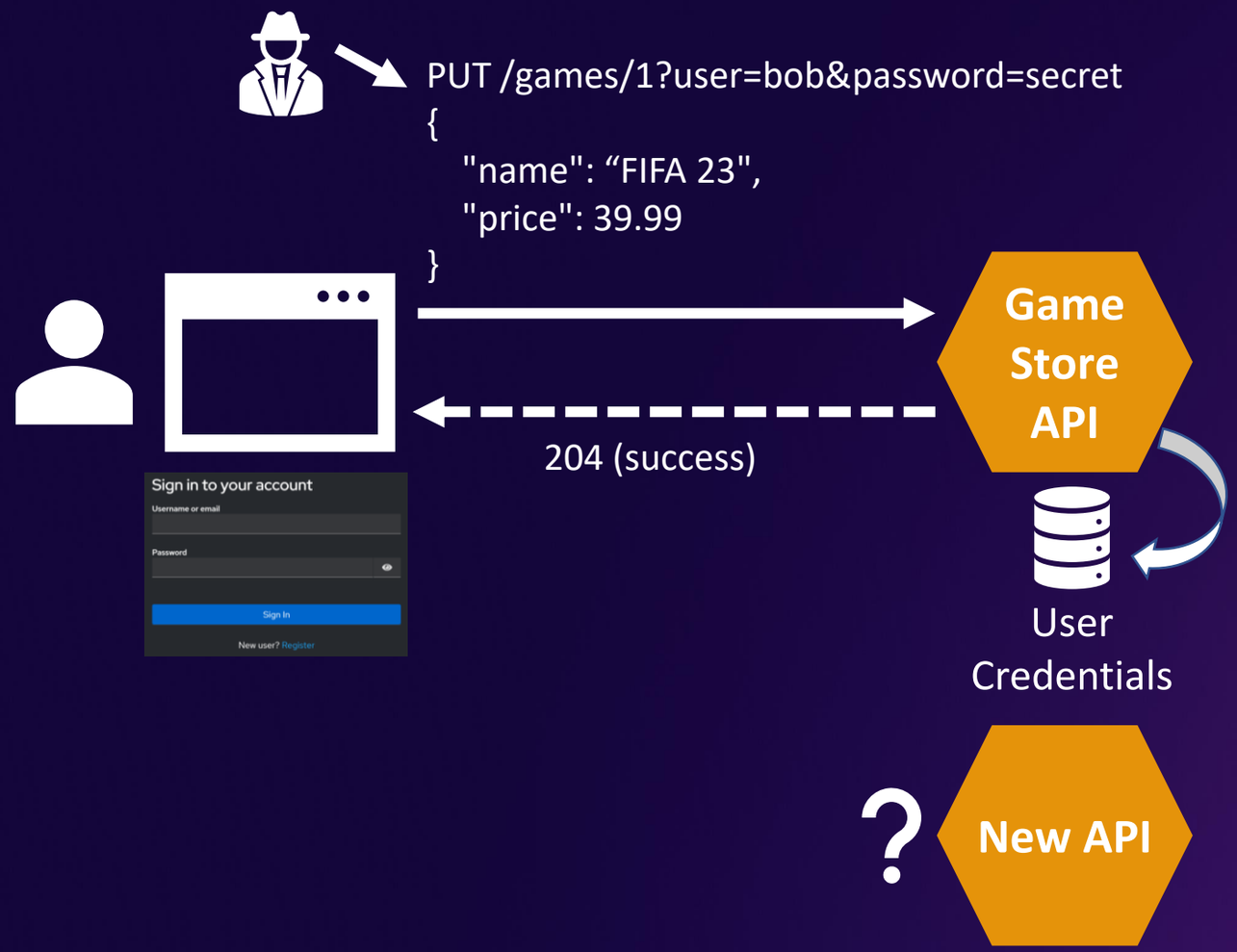
Docker Desktop

https://docs.docker.com/get-started/get-docker

The need for authentication



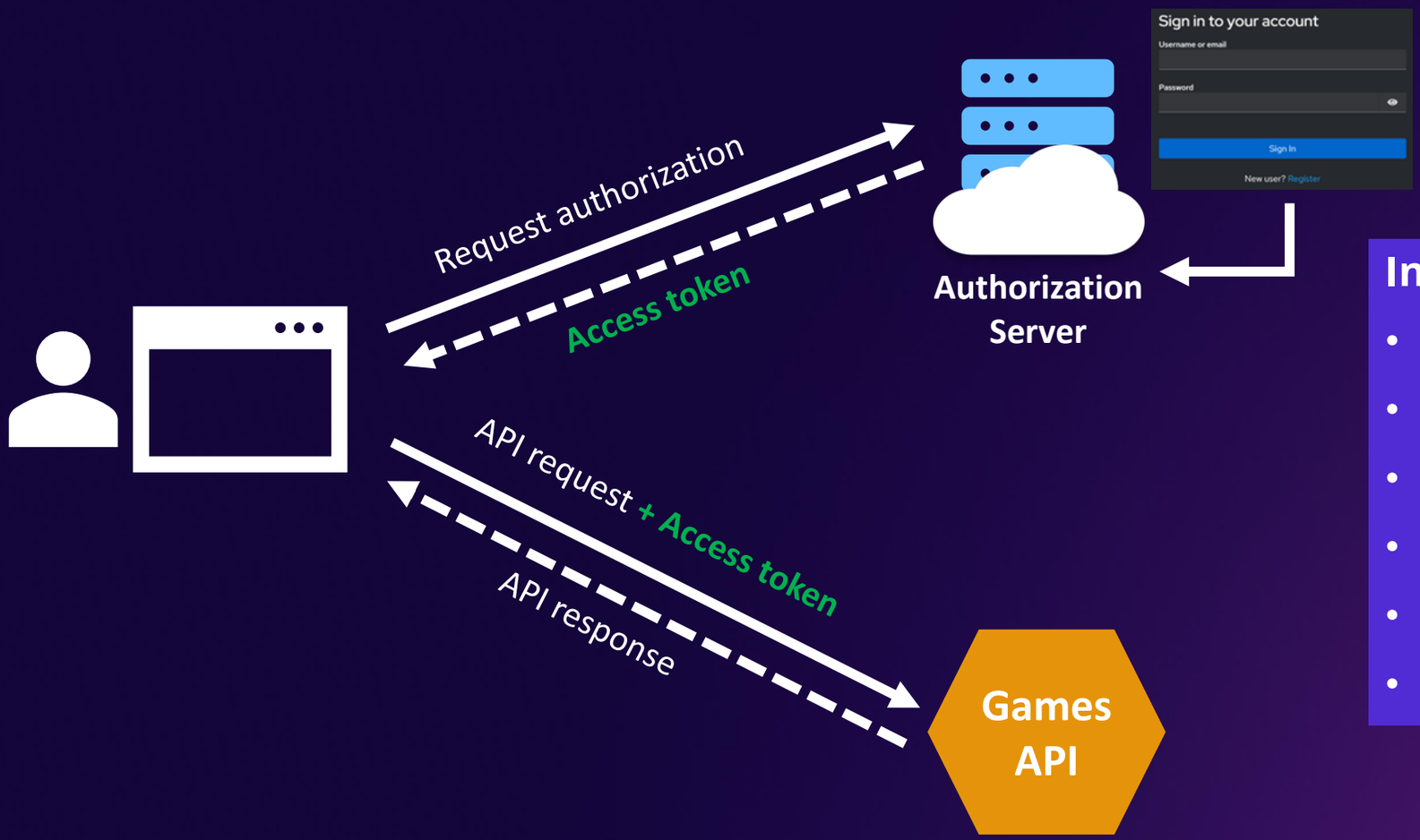
Collect and send user credentials?



ISSUES

- An attacker with a packet sniffer could grab the credentials
- Tools installed on the user’s device could decrypt the URLs
- URLs would get logged on the API
- The client asks for credentials every time or caches them
- Adding a new API presents challenges

What is Token-Based Authentication?



Included in the token

- How to verify it
- Where it came from
- Where it can be used
- Who is authorized
- What can be done with it
- Much more

What is a claim?

A statement about an entity (typically, the user) and additional data

role: admin

aud: http://gamestore-api

exp: 1716140901

What is a JSON Web Token (JWT)?

JSON Web Token (JWT) is a compact, URL-safe means of representing claims to be transferred between two parties.

A signed JWT is known as a JSON Web Signature (JWS)

JSON Web Token (JWT) structure

JWT Header

Field	Sample Value	Description
alg	RS256	Signing algorithm
typ	jwt	Type of token jwt: JSON Web Token
kid	39629176BDF969722B7D83B77500D83C	Identifier of the key used to sign the token

JWT Payload

Field	Sample Values	Description
iss	dotnet-user-jwts http://localhost:8080/realms...	Issuer: Who created and signed the token
aud	http://localhost:5124 gamestore-api	Audience: Who the token is intended for
email	bob@gamestore.com	End-User's preferred e-mail address
sub	julio 167e91a3-fe94-4539-8e66...	Subject. The principal that is the subject of the JWT. The Id of the signed in user.
scope	gamestore_api.all openid profile	The type of access or permissions granted to the client on behalf of the user
name	Bob Johnson	End-User's full name in displayable form
exp	1615100911	Expiration time after which the JWT MUST NOT be accepted for processing
iat	1617140901	The time at which the JWT was issued

Authentication vs Authorization

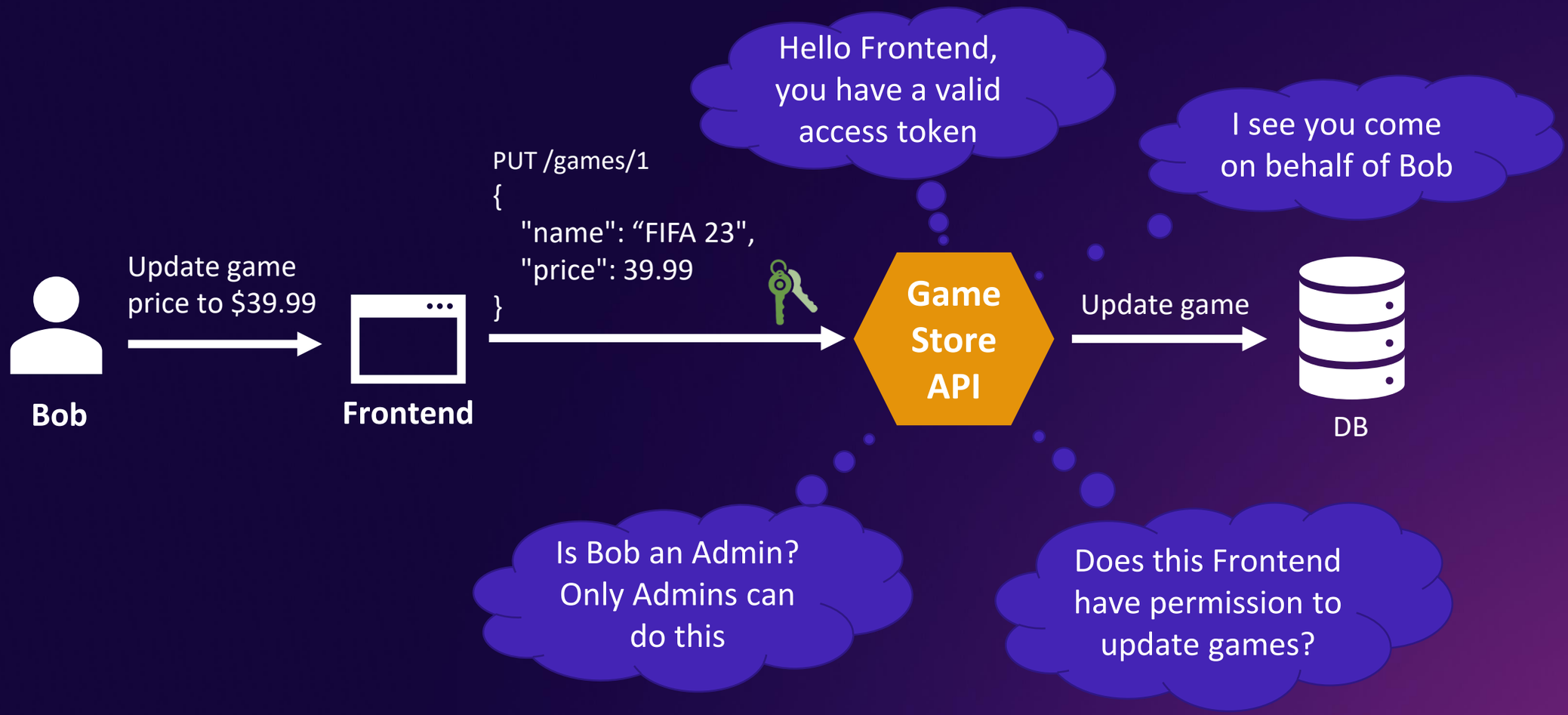
Authentication

The process of verifying the identity of a user or system

Authorization

Determines what an authenticated user or system is allowed to do

The need for authorization



ASP.NET Core authorization types

Role-Based

Checks whether a user has a particular role to determine their permissions

Claims-Based

Uses claims (user or client attributes) to make authorization decisions

Policy-Based

Uses authorization policies to determine if access should be granted

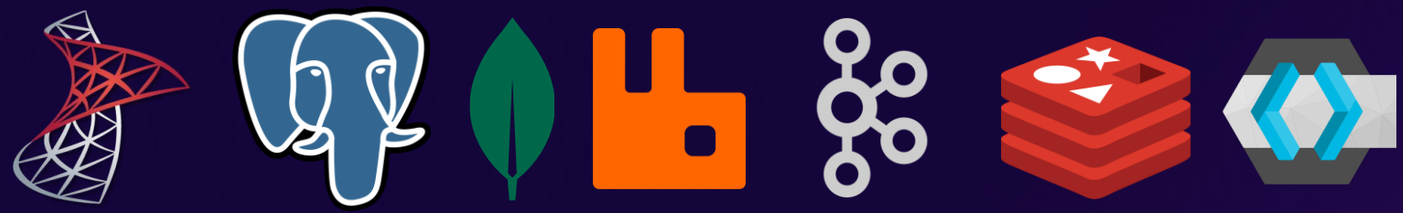
Resource-Based

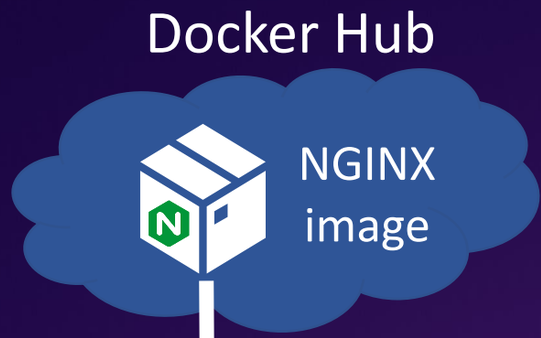
Makes decisions based on the resource being accessed

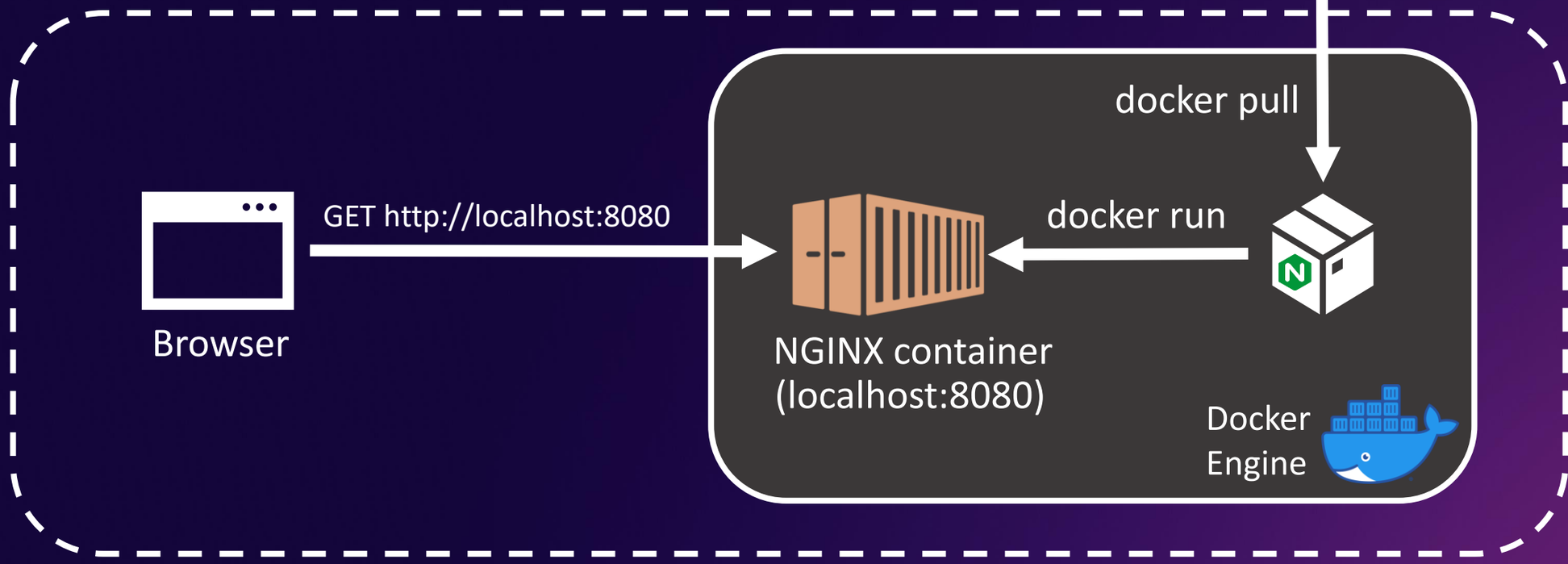
What is Docker?

A platform to package and run applications in loosely isolated environments called containers

Running a Docker image





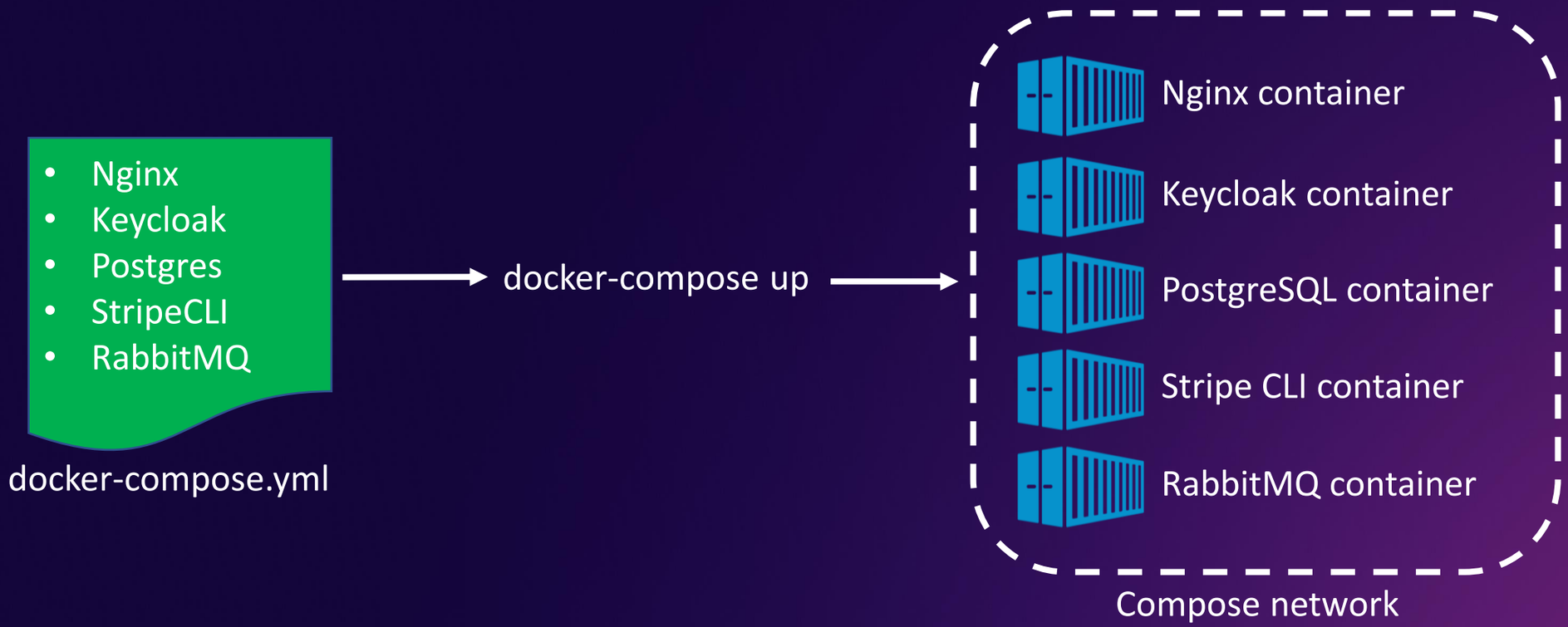


Do I need yet another Docker tool?

- **Too many steps to setup infrastructure services**
- **Too many arguments to remember**

What is Docker Compose?

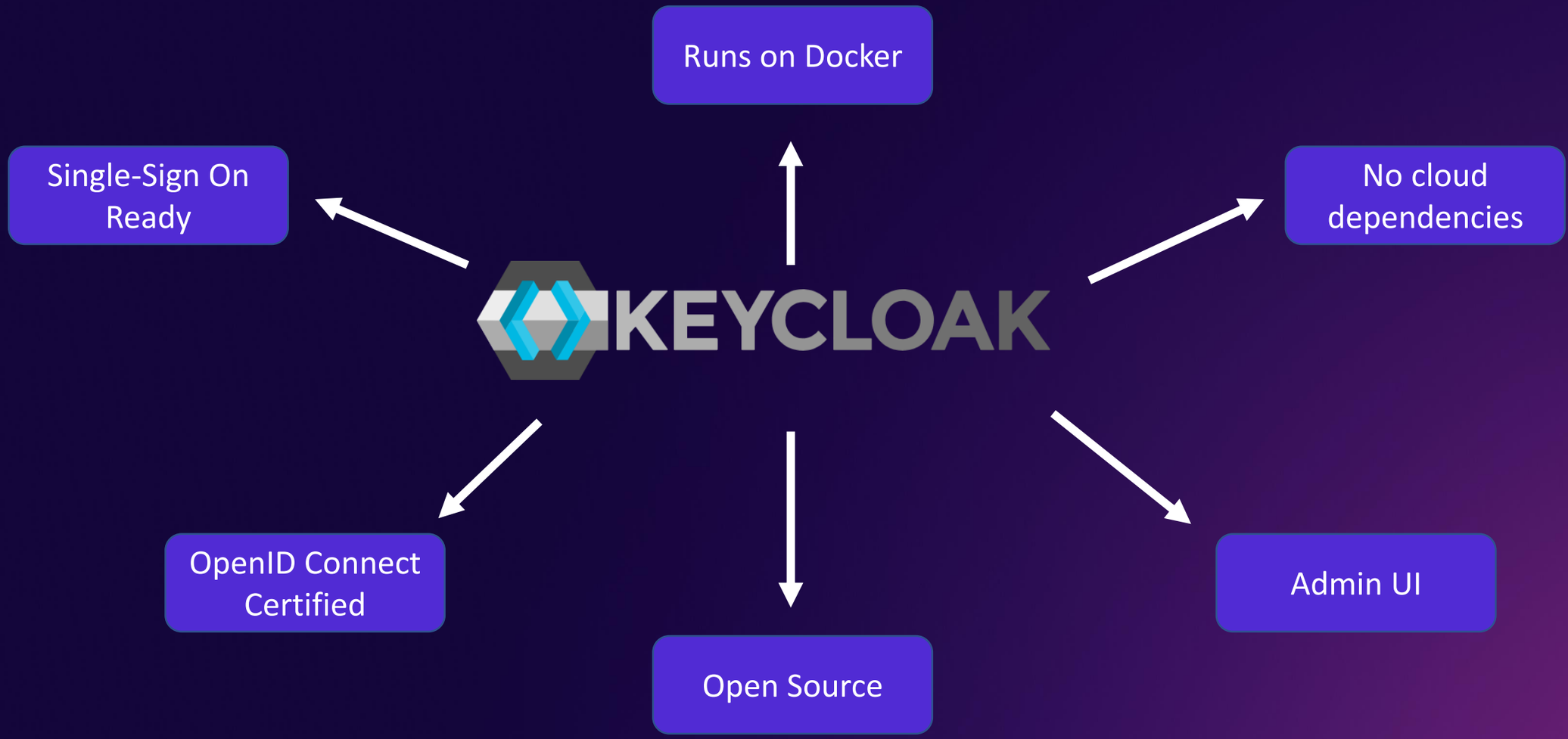
A tool for defining and running multi-container Docker applications



What is Keycloak?

An open-source identity and access management (IAM) tool that helps secure applications and services.

Why Keycloak?



Keycloak as an OpenID Connect Learning Tool

This is not a Keycloak in-depth course

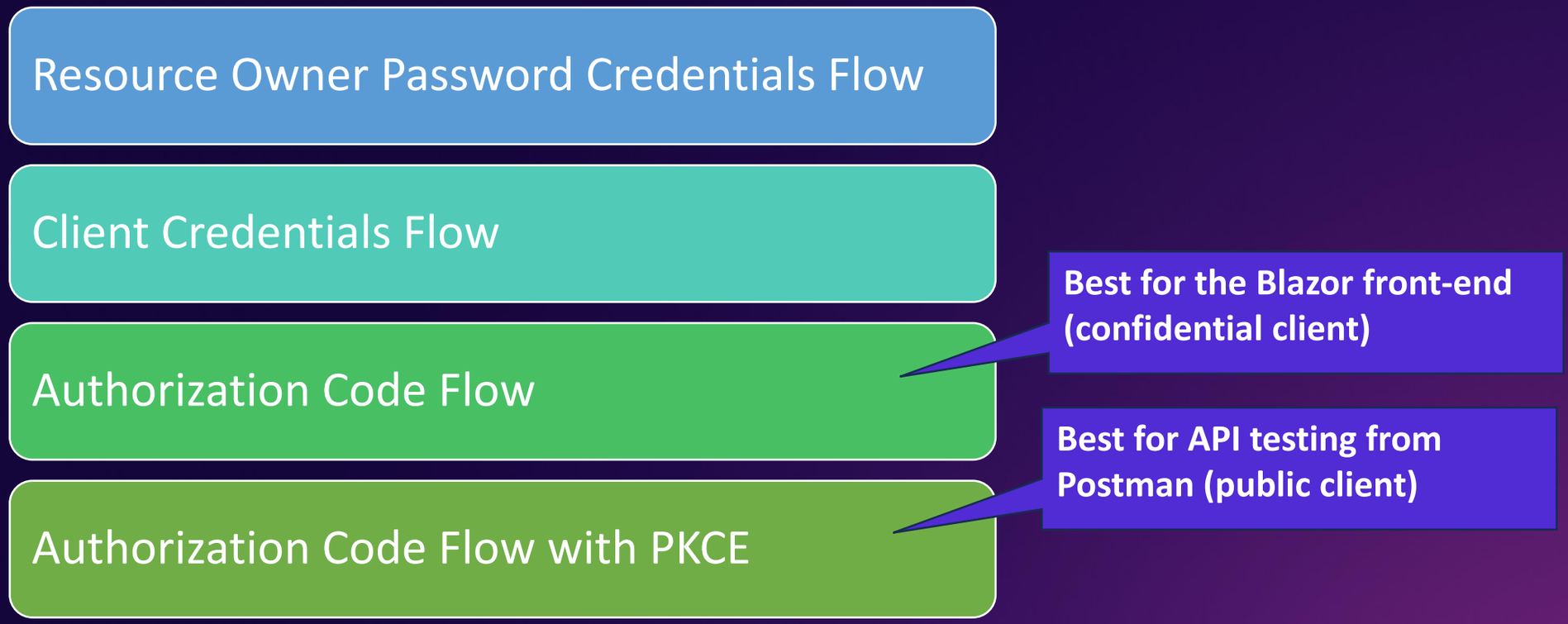
It’s a tool for you to learn OpenID Connect

OpenID Connect will unlock the door to Entra ID and other modern identity providers

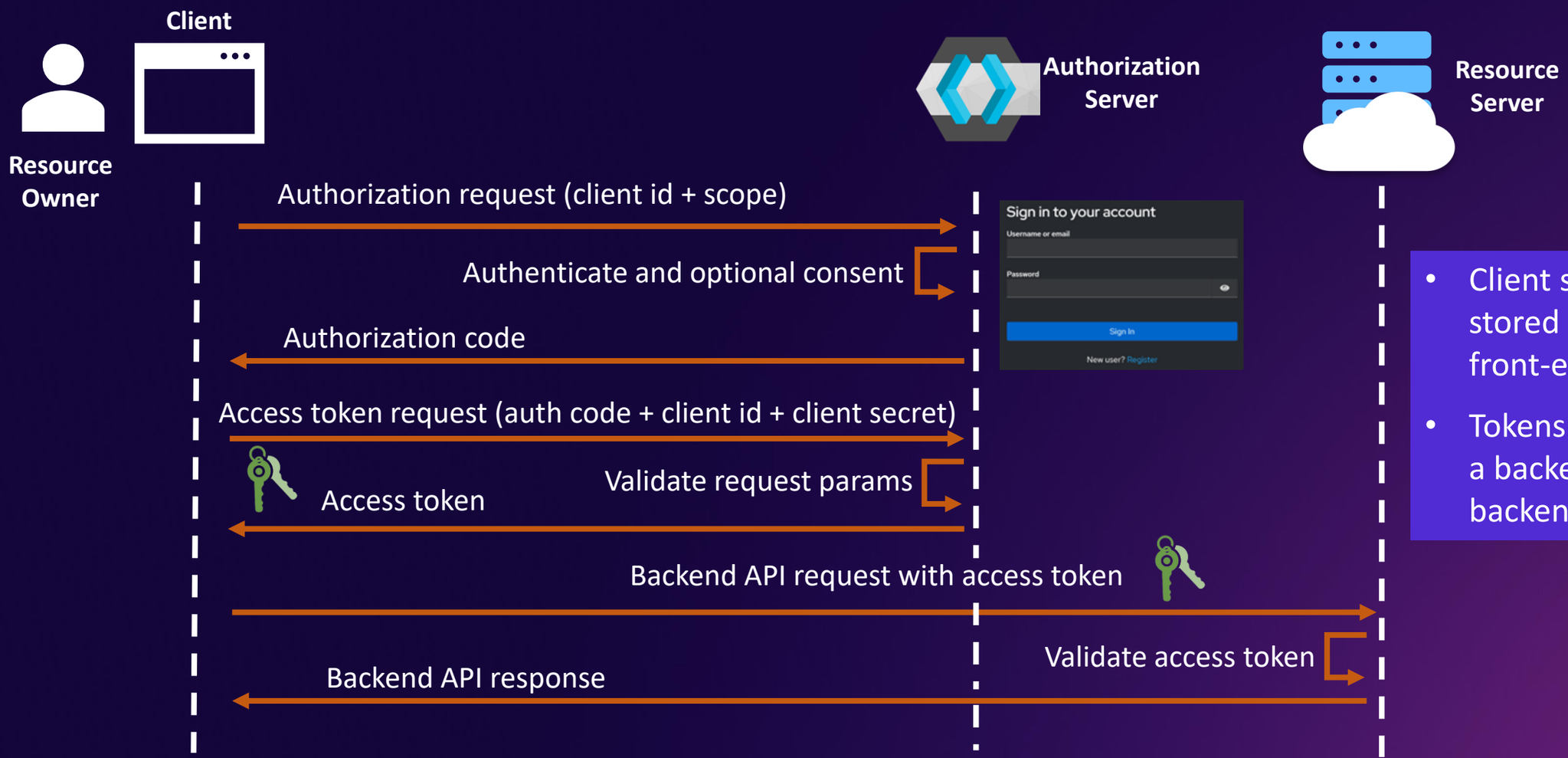
What is OAuth 2.0?

OAuth 2.0 is the industry-standard protocol for authorization, allowing a website or application to access resources hosted by other web apps on behalf of a user

OAuth 2.0 Flows



The Authorization Code Flow

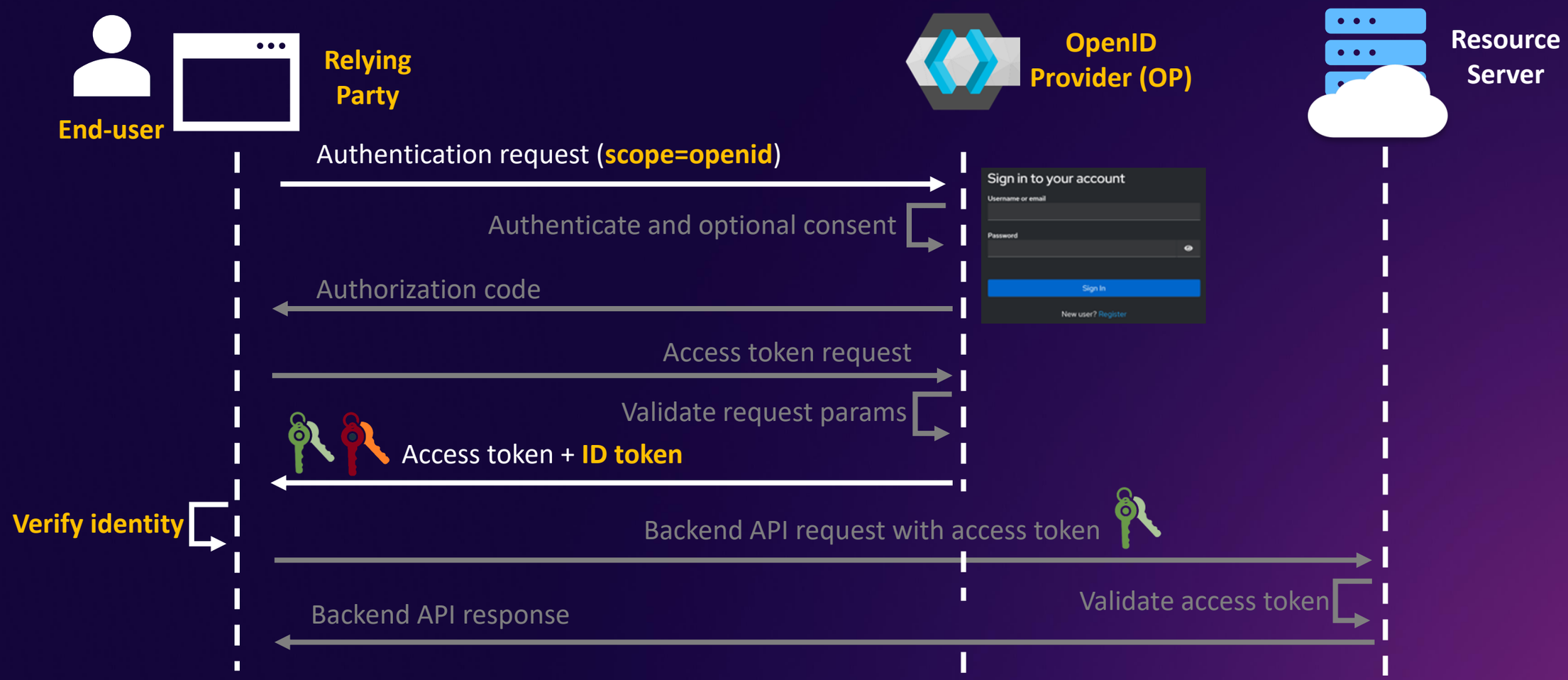


- Client secret safely stored in server-side front-end app
- Tokens obtained via a backend-to-backend request

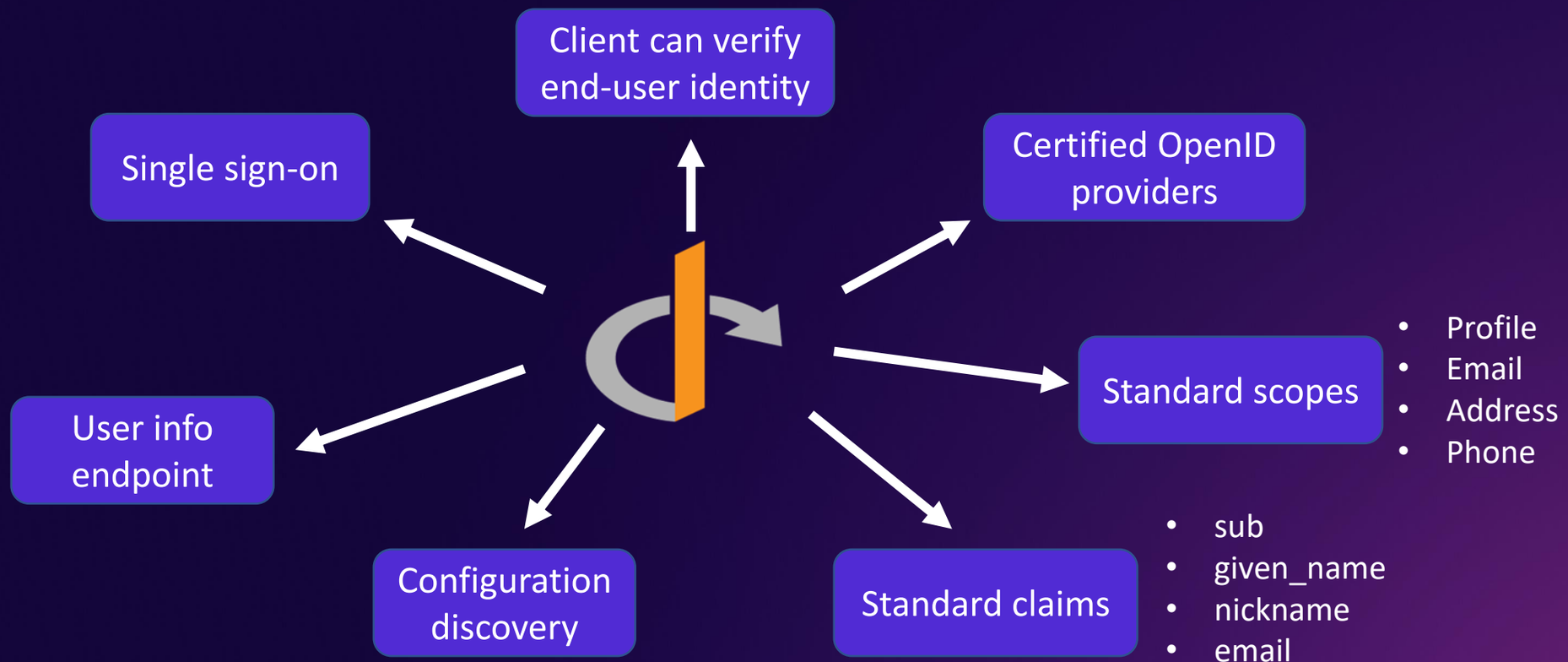
What is OpenID Connect?

OpenID Connect is a simple identity layer on top of the OAuth 2.0 protocol that allows clients to verify the identity of the End-User

The OpenID Connect authentication flow



What OpenID Connect adds



- Profile
- Email
- Address
- Phone

- sub
- given_name
- nickname
- email
- birthdate
- Etc…